

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1 1-38. (Canceled)

1 39. (New): A digital signing method, comprising:

2 computing a hash value of inputted data including a message to be signed or a
3 hash value thereof;

4 encoding the computed hash value of the inputted data to produce encoded data of
5 a predetermined format that is suitable for encryption processing for generating a signature;

6 applying a secret key to the encoded data to generate a digital signature for the
7 message to be signed;

8 registering log data including the generated digital signature on a log list; and

9 distributing a signature-attached data including the generated digital signature for
10 the message to be signed, the message to be signed, and the previous log data or the hash value
11 thereof for generating the signature; and

12 wherein the inputted data used for generating the digital signature further includes
13 another log data or a hash value thereof that has previously been generated and registered on the
14 log list.

1 40. (New): The digital signing method of claim 39, wherein said log data
2 further comprises a distribution destination, and wherein said log data including a distribution
3 destination attached thereto.

1 41. (New): The digital signing method of claim 39, said method further
2 comprising:

3 permitting registration of the log data with said log list only when the data from a
4 previously signed message is included in the latest log data registered with said log list.

1 42. (New): The digital signing method of claim 39, said method further
2 comprising:
3 obtaining a timestamp from a trusted authority, said timestamp generated by
4 applying a second secret key to the digital signature, and a time; and
5 distributing a signature-attached data including the generated digital signature for
6 the message to be signed, the message to be signed, the previous log data or the hash value
7 thereof for generating the signature, and the timestamp.

1 43. (New): A digital signing apparatus, comprising:
2 a processor; and
3 a storage medium, wherein said processor computes a hash value of inputted data
4 including a message to be signed or a hash value thereof, and wherein
5 said processor encodes the computed hash value of the inputted data into encoded
6 data of a predetermined format that is suitable for encryption processing for generating a
7 signature;
8 said processor applies a secret key to the encoded data to generate a digital
9 signature for the message to be signed;
10 said processor prepares a signature-attached data including the generated digital
11 signature for the message to be signed, the message to be signed, and the previous log data or the
12 hash value thereof for generating the signature; and
13 said processor registers log data of said signature-attached data with a log list in
14 said storage medium.

1 44. (New): The digital signing apparatus of claim 43, wherein
2 said processor applies said secret key to a message or the hash value thereof to
3 generate a digital signature for the message; and wherein
4 said processor prepares a signature-attached data that includes the generated
5 digital signature, the message, and the previous log data or hash value thereof; and wherein

6 said processor registers log data of a signature-attached data including the
7 generated digital signature, the message, and the previous log data or hash value thereof, with
8 said log list.

1 45. (New): The digital signing apparatus of claim 43, wherein said log data
2 further comprises a distribution destination.

1 46. (New): The digital signing apparatus of claim 43, wherein:
2 registration of the log data with said log list is permitted only when the previous
3 log data is included in the latest log data registered with said log list.

1 47. (New): The digital signing apparatus of claim 43, wherein:
2 said processor obtains a timestamp from a trusted authority, said timestamp
3 generated by applying a second secret key to the digital signature, and a time; and
4 said processor prepares said signature-attached data including the generated
5 digital signature, the message, and the previous log data or hash value thereof, and the
6 timestamp.

1 48. (New): The digital signing apparatus of claim 43, further comprising: an
2 interface configured to be connectable to a computer.

1 49. (New): The digital signing apparatus of claim 48, wherein:
2 if a number of the log data registered with the log list exceeds a particular value,
3 said processor outputs at least one of a plurality of log data registered with the log list to said
4 computer, whereupon said computer registers said at least one of a plurality of log data with a
5 second log list prepared in said computer, and thereupon,
6 said processor deletes said at least one of a plurality of log data from said log list
7 in said storage medium.

1 50. (New): A computer program product for creating a digital signature, said
2 program product comprising:

3 program code to operate a processor to compute a hash value of inputted data
4 including a message to be signed or a hash value thereof;

5 program code to operate the processor to encode the computed hash value of the
6 inputted data into predetermined format data that is suitable for encryption processing for
7 generating a signature;

8 program code to operate the processor to apply a secret key to the encoded data to
9 generate a digital signature for the message to be signed;

10 program code to operate the processor to register a log data including the
11 generated digital signature on a log list in said storage medium; and

12 a computer readable storage medium for embodying the codes.

1 51. (New): A computer program product of claim 50, wherein the computer
2 readable storage medium is a computer readable medium for storing the codes.

1 52. (New): A computer program product of claim 50, wherein the computer
2 readable storage medium is a computer readable medium for transmitting the codes.